

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-204134

(P2005-204134A)

(43) 公開日 平成17年7月28日(2005.7.28)

(51) Int. Cl. 7

F I

テーマコード (参考)

H04L 9/10
G06F 12/14
G06F 17/60
G09C 1/00

H04L 9/00 621A
G06F 12/14 310Z
G06F 17/60 242
G09C 1/00 660A

5B017
5J104

審査請求 未請求 請求項の数 8 O L (全 10 頁)

(21) 出願番号 特願2004-9134 (P2004-9134)
(22) 出願日 平成16年1月16日 (2004.1.16)

(71) 出願人 000006013
三菱電機株式会社
東京都千代田区丸の内二丁目2番3号
(74) 代理人 100099461
弁理士 溝井 章司
(74) 代理人 100111800
弁理士 竹内 三明
(72) 発明者 三澤 学
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内
(72) 発明者 山田 敬喜
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内
Fターム(参考) 5B017 AA02 BA07 CA14
5J104 AA12 NA35 NA42 PA10 PA12

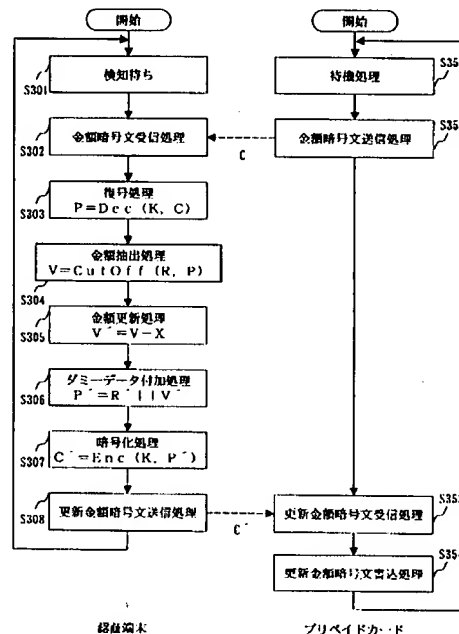
(54) 【発明の名称】 耐タンパ暗号システム及びメモリ装置及び認証端末及び及びプログラム

(57) 【要約】

【課題】 プリペイドカード等のメモリの更新技術に係り、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止することを課題とする。

【解決手段】 認証装置は、メモリ装置から受信した管理データ暗号文を復号し(S303)、そこから先頭の乱数を除去して、金額を抽出する(S304)。そして、消費金額を差し引いて、残高となる更新金額を算出する(S305)。更新金額の先頭にダミーデータとして乱数を付加したのちに(S306)、これを暗号化する(S307)。その暗号結果を、プリペイドカードに書き込む。また、暗号ブロック連鎖モードの暗号方式を採用することも有効である。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を外部より受信する管理データ暗号文受信部と、

受信した前記管理データ暗号文を復号する復号部と、

復号結果から前記ダミーデータを除いて、前記管理データを抽出する管理データ抽出部と、

抽出した前記管理データを更新して更新管理データを生成する管理データ更新部と、

前記更新管理データに新たなダミーデータを付加するダミーデータ付加部と、

前記新たなダミーデータが付加された更新管理データを暗号化して更新管理データ暗号文を生成する暗号化部と、

前記更新管理データ暗号文を外部へ送信する更新管理データ暗号文送信部とを有することを特徴とする認証端末。

【請求項 2】

ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を保持するメモリ装置であって、

前記管理データ暗号文を記憶する管理データ暗号記憶部と、

該管理データ暗号記憶部で記憶している前記管理データ暗号文を外部へ送信する管理データ暗号文送信部と、

外部から新たなダミーデータが付加された更新された管理データが秘匿状態に変換された更新管理データ暗号文を受信する更新管理データ暗号文受信部と、

受信した前記更新管理データ暗号文を前記管理データ暗号記憶部に書き込む更新管理データ暗号文書込部と

を有することを特徴とするメモリ装置。

【請求項 3】

メモリ装置は、プリペイドカード、RFID（電波方式認識）カード、あるいはICカードのいずれか、または不揮発メモリを有した端末であって、

管理データは、金額、量、回数、または度数であることを特徴とする請求項 2 記載のメモリ装置。

【請求項 4】

ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を保持するメモリ装置と、前記管理データを更新する認証端末とからなり、互いに通信可能な耐タンパ暗号システムであって、

前記メモリ装置は、前記管理データ暗号文を記憶する管理データ暗号記憶部と、

該管理データ暗号記憶部で記憶している前記管理データ暗号文を前記認証端末へ送信する管理データ暗号文送信部とを有し、

前記認証端末は、前記メモリ装置から前記管理データ暗号文を受信する管理データ暗号文受信部と、

受信した前記管理データ暗号文を復号する復号部と、

復号結果から前記ダミーデータを除いて、前記管理データを抽出する管理データ抽出部と、

抽出した前記管理データを更新して更新管理データを生成する管理データ更新部と、

前記更新管理データに新たなダミーデータを付加するダミーデータ付加部と、

前記新たなダミーデータが付加された更新管理データを暗号化して更新管理データ暗号文を生成する暗号化部と、

前記更新管理データ暗号文を前記メモリ装置へ送信する更新管理データ暗号文送信部とを有し、

前記メモリ装置は、更に、前記認証端末から前記更新管理データ暗号文を受信する更新管理データ暗号文受信部と、

受信した前記更新管理データ暗号文を前記管理データ暗号記憶部に書き込む更新管理デ

10

20

30

40

50

ータ暗号文書込部と
を有することを特徴とする耐タンパ暗号システム。

【請求項 5】

メモリ装置は、プリペイドカード、R.F I D（電波方式認識）カード、あるいは I C カードのいずれか、または不揮発メモリを有した端末であって、

管理データは、金額、量、回数、または度数であることを特徴とする請求項 4 記載の耐タンパ暗号システム。

【請求項 6】

ダミーデータ付加部は、乱数を取得し、取得した乱数をダミーデータとして、更新管理データの先頭に付加し、

管理データ抽出部は、復号した平文から先頭のダミーデータを除いて、管理データを抽出することを特徴とする請求項 4 記載の耐タンパ暗号システム。

【請求項 7】

暗号化部は、暗号ブロック連鎖モードの暗号化を行い、

復号部は、暗号ブロック連鎖モードの復号を行うことを特徴とする請求項 4 記載の耐タンパ暗号システム。

【請求項 8】

管理データを秘匿状態に変換した管理データ暗号文を保持するメモリ装置と通信して、管理データを更新する認証装置となるコンピュータに、

メモリ装置から前記管理データ暗号文を受信する手順と、

受信した前記管理データ暗号文を復号する手順と、

復号した平文からダミーデータを除いて、管理データを抽出する手順と、

抽出した管理データを更新して更新管理データを生成する手順と、

更新管理データにダミーデータを付加する手順と、

ダミーデータを付加して得られた平文を、暗号化する手順と、

暗号の結果として得られた更新管理データ暗号文をメモリ装置へ送信する手順とを実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、プリペイドカードや R F I D（Radio Frequency Identification：電波方式認識）や I C カード、不揮発メモリを有した端末等のメモリの更新技術に係り、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止する技術に関する。

【背景技術】

【0002】

本発明は、例えば、プリペイドカードや R F I D や I C カード、不揮発メモリを有した端末のように、サービスを提供する際にメモリに書き込まれている残高から使用額を減算し、その残高をカード等へ書き込む方式等に関する。

【0003】

残高をそのままカードへ書き込むと、メモリのリーダライタや通信部分を擬似する装置があれば簡単にカードを偽造することが可能である。その為、暗号を用いて、残高を暗号化して書き込むことにより改ざんを防止している。

【0004】

図 8 は、従来の処理フローを示す図である。認証端末 1 で、プリペイドカード 2 を検知すると、プリペイドカード 2 から暗号化されている金額を読み込む（S 8 0 2）。そして、復号してから（S 8 0 3）、金額等を更新し（S 8 0 4）、その後暗号化して（S 8 0 5）、プリペイドカード 2 に書き込む（S 8 0 6）ように動作している。

【0005】

しかし認証端末に対してサイドチャネルアタックができるような場合には、これだけで

10

20

30

40

50

は安全といえない。残高を暗号化する際の消費電力や電磁波等を観測し、サイドチャネルアタックによって暗号の秘密鍵を解析される可能性がある。

【発明の開示】

【発明が解決しようとする課題】

【0006】

本発明は、上記した従来技術の欠点を除くためになされたものであって、その目的とするところは、プリペイドカード等のメモリの更新技術に係り、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止することである。

【課題を解決するための手段】

【0007】

10

本発明に係る認証端末は、

ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を外部より受信する管理データ暗号文受信部と、

受信した前記管理データ暗号文を復号する復号部と、

復号結果から前記ダミーデータを除いて、前記管理データを抽出する管理データ抽出部と、

抽出した前記管理データを更新して更新管理データを生成する管理データ更新部と、

前記更新管理データに新たなダミーデータを付加するダミーデータ付加部と、

前記新たなダミーデータが付加された更新管理データを暗号化して更新管理データ暗号文を生成する暗号化部と、

20

前記更新管理データ暗号文を外部へ送信する更新管理データ暗号文送信部とを有することを特徴とする。

【発明の効果】

【0008】

本発明においては、金額である平文に乱数等のダミーデータ付加して暗号化するので、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止することができる。その他の効果として、同じ金額（量・回数・度数）を書いたとしても乱数等のダミーデータによって書き込む暗号文は毎回異なり、金額（量・回数・度数）を予想できないという効果もある。

【発明を実施するための最良の形態】

30

【0009】

実施の形態1.

以下本発明を図面に示す実施例に基づいて説明する。図1は、想定環境を示す図である。この例では、プリペイドカードと、更新する認証端末を例としているが、更新対象である管理データ（特に、度数、回数などの数値の適用が多い）を、メモリに記憶し、その値を第三者の読み取り、改ざんから防御するシステムに適用可能である。例えば、RFIDやICカード、不揮発メモリを有した端末等にも適用可能である。

【0010】

本発明では、サイドチャネルアタックの対策として、暗号化する際に平文の先頭にダミーデータ（例えば、乱数）を挿入することを特徴とする。

40

【0011】

まず、構成について説明する。図2は、モジュール構成を示す図である。認証端末1は、金額暗号文受信部101、復号部102、金額抽出部103、金額更新部104、ダミーデータ付加部105、暗号化部106、及び更新金額暗号文送信部107を有している。プリペイドカード2は、金額暗号文記憶部201、金額暗号文送信部202、更新金額暗号文受信部203、及び更新金額暗号文書込部204を有している。

【0012】

次に、処理について説明する。図3は、処理フローを示す図である。認証端末1は、プリペイドカード2を検知すると（S301）、金額暗号文受信部101で、プリペイドカード2の金額暗号文送信部202から送信される金額暗号文（金額を暗号化したデータ）

50

を受信する (S302)。

【0013】

そして、復号部102でこれを復号処理する (S303)。このとき、内部で予め秘密状態で記憶している暗号鍵を用いる。

【0014】

そして、金額抽出部103で、金額抽出処理 (S304) する。復号により得られる平文Pからダミーデータを除去して、金額Vを抽出する。例えば、データの先頭部分wのダミーデータをNULLにして、後の金額部分のみが有効なデータに書き換える。尚、図中で、CutOff (X, Y) は、YからXを削除する関数を意味している。

【0015】

次に、金額更新部104で、金額更新処理 (S305) する。金額Vから支払い金額Xを引いて、残額V'を得る。残額V'が、更新される金額となる。

【0016】

ダミーデータ付加部105で、ダミーデータ付加処理 (S306) する。この処理で、更新金額V'に、ダミーデータ (例えば、乱数) を付加する。例えば、更新金額V'の先頭に、ダミーデータを付加する。尚、図中で、X || Y は、XとYを連結する処理を示している。乱数のように、都度異なる値を用いることが有効である。

【0017】

暗号化部106で、ダミーデータが付加された更新金額を平文P'として、暗号化処理 (S307) する。

【0018】

こうして、暗号化された更新金額の暗号文C'を更新金額暗号文送信部107からプリペイドカード2に送信する (S308)。

【0019】

プリペイドカード2では、これを更新金額暗号文受信部203で受信 (S353) し、更新金額暗号文書込部204は、受信した更新金額暗号文C'で、金額暗号文記憶部201の値を更新する (S354)。

【0020】

このように毎回異なる乱数から暗号化を始めることになり、暗号化途中での値を想定させないようにできる。従って、DPA (Differential Power Analysis) 等によるサイドチャネルアタックが困難になる。

【0021】

実施の形態2。

本発明は、上述の例以外にも、部分的に乱数を挿入しても、復号するときにその挿入した乱数の値を知らなくても復号できる方式 (例えば、共通鍵ブロック暗号のCBCモードや公開鍵暗号) に適用できる。

【0022】

本実施の形態では、暗号ブロック連鎖 (CBC: Cipher Block Chaining) モードの暗号化と復号を用いる形態を説明する。

【0023】

まず、暗号化について説明する。実施の形態1のダミーデータ付加部105と暗号化部106の処理に対応する。図4は、CBCモードに適用した場合の暗号化に係るブロックを示す図である。図5は、CBCモードに適用した場合の暗号化に係る処理フローを示す図である。これらの図を用いて、処理を説明する。

【0024】

暗号化される平文P'は、乱数Rと、M1, M2, ...の実データのブロックから構成されている。そして、この先頭ブロックから順に以下の処理を繰り返す (S501)。

【0025】

先頭から順に、平文データのブロックを取得する (S502)。最初は、Rを得る。二回目以降は、M1, M2, ...の順に取得する。これは、論理演算 (401, 402, 40

10

20

30

40

50

3, ...) の一方の入力となる。

【0026】

他の入力データとなる入力側パラメータも特定する (S503)。最初は、乱数IV (ダミーデータに相当) を用いる。二回目以降は、前回の暗号結果 (順に、C0', C1', ...) を用いる。

【0027】

そして、これらの入力側論理演算 (S504) を行う。この例は、排他的論理和 (XOR) を求めている。図4の401, 402, 403に示す処理である。

【0028】

演算結果 (最初は、R', 順にM1', M2', ...) を内部で記憶している暗号鍵 u k e y で暗号化する (S505)。その結果として、順にC0', C1', C2', ... を得る。

【0029】

暗号結果と、復号側と共通して用いる乱数FVを入力として、出力側論理演算する (S506)。この例は、排他的論理和 (XOR) を求めている。図4の421, 422, 423に示す処理である。

【0030】

そして、演算結果を暗号データのブロックとして順に記憶する (S507)。順に、C0, C1, C2, ... となる。

【0031】

すべてのブロックを処理した時点で終了する (S508)。

【0032】

続いて、復号について説明する。実施の形態1の復号部102と金額抽出部103の処理に対応する。図6は、CBCモードに適用した場合の復号に係るブロックを示す図である。図7は、CBCモードに適用した場合の復号に係る処理フローを示す図である。

【0033】

暗号データは、C0, C1, C2, ... のブロックから構成されている。そして、この先頭ブロックから順に以下の処理を繰り返す (S701)。

【0034】

先頭から順に、暗号データのブロックを取得する (S702)。これは、論理演算 (601, 602, 603, ...) の一方の入力となる。

【0035】

他方の入力データとして、暗号側と共通して用いる乱数FVを用いて、入力側論理演算 (S703) を行う。この例は、排他的論理和 (XOR) を求めている。図6の601, 602, 603に示す処理である。

【0036】

演算結果 (最初は、C0', C1', C2', ...) を内部で記憶している暗号鍵 u k e y で復号する (S704)。その結果として、順にR', M1', M2', ... を得る。復号結果は、出力側論理演算の一方の入力となる。

【0037】

他の入力となる出力側パラメータを特定する (S705)。最初は、乱数IV (ダミーデータに相当) を用いる。二回目以降は、前回の復号入力データ (順に、C0', C1', ...) を用いる。

【0038】

そして、これらの出力側論理演算 (S706) を行う。この例は、排他的論理和 (XOR) を求めている。図6の611, 612, 613に示す処理である。

【0039】

演算結果を平文データのブロックとして順に記憶する (S707)。順に、R, M1, M2, ... となる。但し、ダミーデータである乱数Rは、無視して、M1以降のブロックを用いる。

【0040】

乱数Rは1ブロック分でなくても構わない。2ブロック分でも、1ブロックより少なくとも本発明に適用可能である。つまり、乱数がどの部分であるかということさえわかればよい。また乱数を挿入するブロックも1ブロック目でなくても、2ブロック目や3ブロック目でも構わない。また、RSAなどの共通鍵暗号方式の場合には、ブロックは関係なくなり、乱数もどの位置に入れても、乱数の位置さえわかればよい。これは、実施の形態1についても同様である。

【0041】

すべてのブロックを処理した時点で終了する(S708)。

【0042】

10

認証端末1は、コンピュータであり、各要素はプログラムにより処理を実行することができる。また、プログラムを記憶媒体に記憶させ、記憶媒体からコンピュータに読み取られるようにすることができる。

【0043】

図9は、認証端末のハードウェア構成例を示す図である。バスに、演算装置901、データ記憶装置902、メモリ903、通信インターフェース904が接続されている。データ記憶装置902は、例えばROM(Read Only Memory)やハードディスクである。メモリ903は、通常RAM(Random Access Memory)である。

【0044】

20

プログラムは、通常データ記憶装置902に記憶されており、メモリ903にロードされた状態で、順次演算装置901に読み込まれ処理を行う。金額等のデータの受信や送信は、通信インターフェース904により行う。

【図面の簡単な説明】

【0045】

【図1】想定環境を示す図である。

【図2】モジュール構成を示す図である。

【図3】処理フローを示す図である。

【図4】CBCモードに適用した場合の暗号化に係るブロックを示す図である。

【図5】CBCモードに適用した場合の暗号化に係る処理フローを示す図である。

30

【図6】CBCモードに適用した場合の復号に係るブロックを示す図である。

【図7】CBCモードに適用した場合の復号に係る処理フローを示す図である。

【図8】従来の処理フローを示す図である。

【図9】認証端末のハードウェア構成例を示す図である。

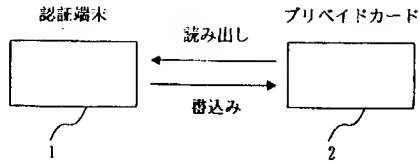
【符号の説明】

【0046】

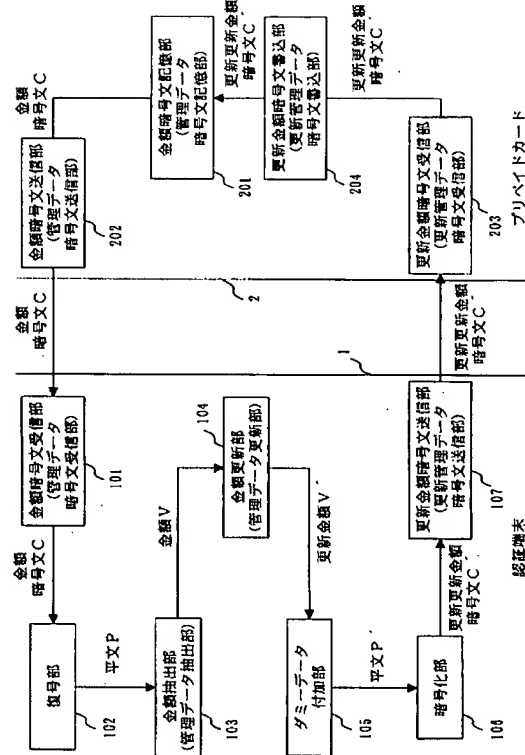
1 認証端末、2 プリペイドカード、101 金額暗号文受信部、102 復号部、103 金額抽出部、104 金額更新部、105 ダミーデータ付加部、106 暗号化部、107 更新金額暗号文送信部、201 金額暗号文記憶部、202 金額暗号文送信部、203 更新金額暗号文受信部、204 更新金額暗号文書込部。

40

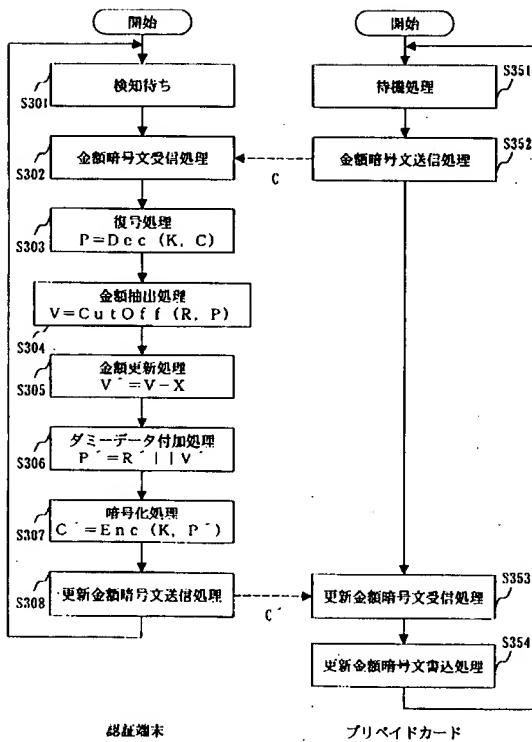
【図 1】



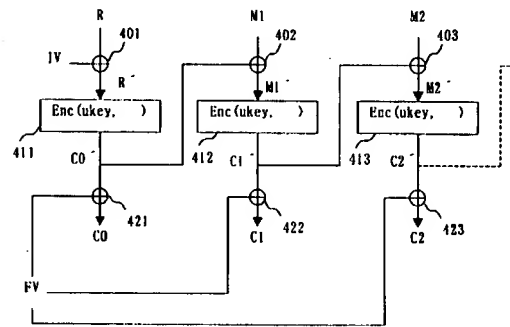
【図 2】



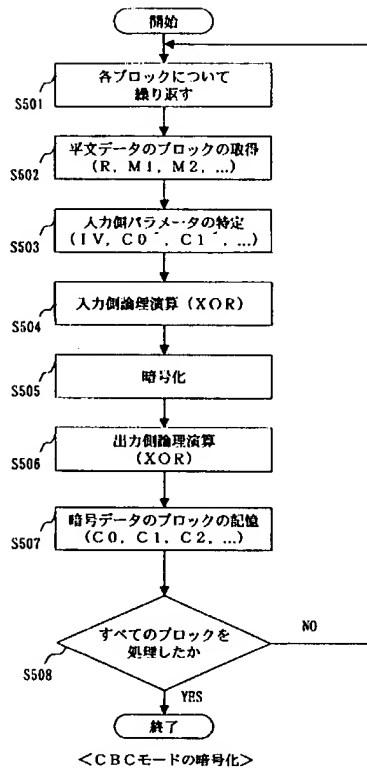
【図 3】



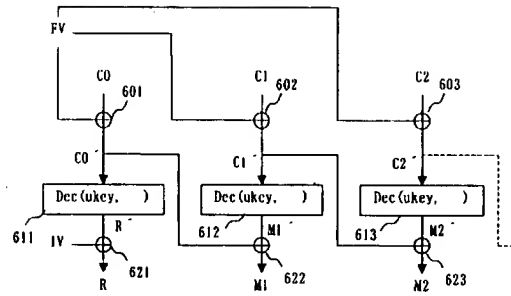
【図 4】



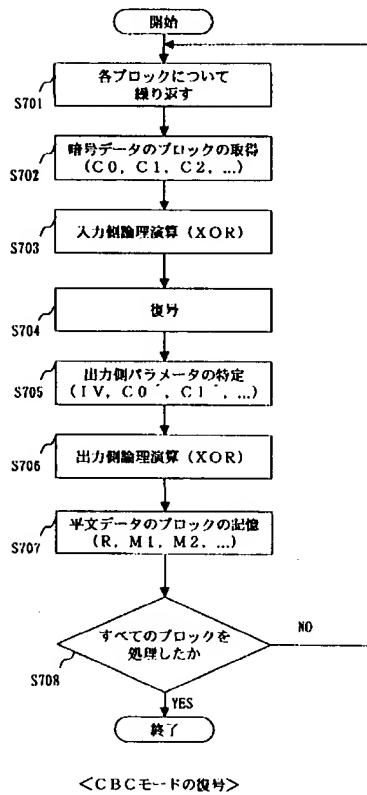
【図 5】



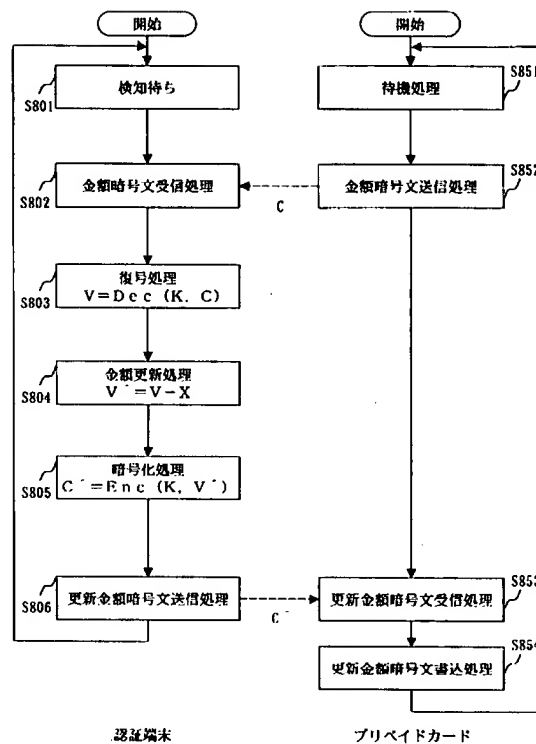
【図 6】



【図 7】



【図 8】



【図 9】

